



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/356,600	07/19/1999	WILLIAM DUANE	SDT-040	8046
21323	7590	10/06/2003	EXAMINER	
TESTA, HURWITZ & THIBEAULT, LLP			ARANI, TAGHI T	
HIGH STREET TOWER			ART UNIT	PAPER NUMBER
125 HIGH STREET			2131	
BOSTON, MA 02110			DATE MAILED: 10/06/2003	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/356,600	DUANE ET AL.
	Examiner	Art Unit
	Taghi T. Arani	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 19 July 1999.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-51 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-19,21-29,32-34,36-39,42-51 is/are rejected.

7) Claim(s) 20,30,31,35,40 and 41 is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) The proposed drawing correction filed on _____ is: a) approved b) disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.

2. Certified copies of the priority documents have been received in Application No. _____.

3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) The translation of the foreign language provisional application has been received.

15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5,6.

4) Interview Summary (PTO-413) Paper No(s). _____.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____.

DETAILED ACTION

Claims 1-51 were pending for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1, It would not be clear to one of ordinary skill in the art whether “receiving information” recited in step (a) is from the same entity (provider) as that of “receiving authentication information” recited in step (c) or from different entities (providers) and whether “providing” recited in steps (b) and (d) is to the same entity (receiver) or different entities (receivers).

Dependent claims 2-10 are also rejected by virtue of their dependencies.

As per claim 11, It would not be clear to one of ordinary skill in the art whether “receiving” recited in step (a) is by the same entity (receiver) as that of “receiving” recited in step (b) or different entities (receiver) and who is “decrypting ...personal security device”.

Dependent claims 12-18 are also rejected by virtue of their dependencies.

Claims 42-51 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 42 recites the limitation "said personal security device" in line 4. There is insufficient antecedent basis for this limitation in the claim. For the purpose of applying art, the examiner assumes "said encrypted personal security device" as recited in line 3.

Dependent claims 43-51 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 5-7, 9, 11, 25-29, 33-34, 36, 39, 42, 44-47, 49-50 are rejected under 35 U.S.C. 102(e) as being anticipated by Holloway, U.S. Pat. No. 6,424,718 filed June 1997.

As per claims 1-2, 11, 25, 33 and 42, Holloway is directed to a communication system for processing messages using public key cryptography with a private key unique to one or more users. Holloway's system comprises; server means adapted for data communication with a client via a network, see col. 3, lines 27-51.

In a preferred embodiment, Holloway discloses that a private key (i.e. a personal security device) of a user is stored in a storage portion of a key server or written to a data storage means to which the server has access. The private key is delivered from server system to a user within an applet Ap via web server and World Wide Web (WWW), see col. 7, lines 30-67.

In operation, when a user claiming to be authorized accesses a WWW page on the web server via a browser on a client. The server compiles the applet Ap which includes the claimed

users encrypted private key (i.e. encrypted personal security device) stored on the key server, and all of the associated cryptographic algorithms. The server sends (i.e. providing the encrypted personal security device) the applet to the browser. At the browser, the private key is decrypted if the claimed user knows the owning pass phrase (PPu) which establishes the identity of the owning user (i.e. if the user is authenticated).

Holloway teaches that transaction is secured by applet Ap through steps of user Registration, User sign in; User authentication, Message security, User re-registration, and Revocation. Holloway teaches that SSL (secure socket layer) may be employed to establish the authenticity of server.

Holloway teaches that in the user sign in step, user enters his identity to client whereby the identity is sent by applet Ap to server system in enciphered form. The server returns the encrypted private key record with respect to registration stage. The applet AP requests user to enter the pas-phrase PPu (i.e. authentication information). Holloway teaches that then private key is made available to user only if the user sign in details and pass-phrase PPu received by applet Ap is correct an the user is authentic, see col. 9, lines 10-38.

Holloway's communications system comprises a client computer coupled to a World Wide Web (WWW) implementing a modem link, local area network (LAN), wide area network (WAN) or any combination. The client computer of Holloway comprises a web browser and a smart card reader. Holloway discloses that coupled to WWW is a web server coupled to a key server through a firewall, see col. 6, lines 13-41, see also Fig.1.

Holloway teaches that the PPu (i.e. authentication information) could be stored in a smart card, see col. 8, lines 22-23.

As per claim 3, Holloway's private key is doubly encrypted using PPu and a Consent phrase (CPu), see col. 8, lines 38-42 which provides an encrypted communication between the client and the key server , see col. 8, line 66 through col. 9, line 1.\, see also col. 9, lines 16-26, col. 7, lines 45-47..

As per claim 5, Holloway teaches that in the user sign in step, user enters his identity to client whereby the identity is sent by applet Ap to server system in enciphered form. The server returns the encrypted private key record with respect to registration stage. The applet AP requests user to enter the pas-phrase PPu (i.e. authentication information). Holloway teaches that then private key is made available to user only if the user sign in details and pass-phrase PPu received by applet Ap is correct an the user is authentic, see col. 9, lines 10-38.

As per claim 6, encrypted private key of Holloway is retrieved by the key server and is provided to the Applet Ap, see col. 8, lines 40-44, line 66 through col. 8, line10, see also col. 7, lines 30-47.

As per claim 7, the system server of Holloway stores, retrieves the encrypted private key and authenticates the identity of the user desiring access to the network (i.e. the system server constitutes recited authentication server).

As per claim 9, Holloway teaches that when applet Ap or browser terminate, the algorithm and keys are lost from the memory of client (i.e. stored information in volatile memory)

Claims 25-27 are apparatus corresponding to method claims 1-3. Claims 25-27 are rejected for the same reasons provided in the statement of rejection of claims 1-3.

As per claim 28, Holloway's private key is doubly encrypted using PPu and a Consent phrase (CPu), see col. 8, lines 38-42 which provides an encrypted communication between the

client and the key server, see col. 8, line 66 through col. 9, line 1, see also col. 9, lines 16-26, col. 7, lines 45-47.

Claim 29 is an apparatus corresponding to method claim 7. Claim 29 is rejected for the same reason provided in the rejection of claims 7 above.

As per claims 33, 36 and 39, Holloway teaches that in the user sign in step, user enters his identity to client whereby the identity is sent by applet Ap to server system in enciphered form. The server returns the encrypted private key record with respect to registration stage. The applet AP requests user to enter the pas-phrase PPu (i.e. authentication information). Holloway teaches that then private key is made available to user only if the user sign in details and pass-phrase PPu received by applet Ap is correct an the user is authentic, see col. 9, lines 10-38.

The teaching of Holloway clearly suggest a client (with a first receiver and a first transmitter) connected to the key server for transmitting client identity and receiving encrypted personal security device (i.e. encrypted private key) and a second receiver (such as smart card reader for receiving the PPu) and a second transmitter for transmitting the PPu to the client. A decryptor decrypting personal security device is inherent in Holloway's applet Ap supporting steps of User registration, User log in, User authentication, Message security and SSL.

Furthermore, Holloway teaches that the PPu (i.e. decryption information) may be stored on a smart card (recited in claim 39), see 8, line 21-23.

As per claim 34, Holloway's private key is doubly encrypted using PPu and a Consent phrase (CPu), see col. 8, lines 38-42 which provides an encrypted communication between the client and the key server, see col. 8, line 66 through col. 9, line 1, see also col. 9, lines 16-26, col. 7, lines 45-47.

As per claim 44, Holloway teaches that the encrypted private key is stored in a memory at the key server of server system and the private key is indexed to the identity of the user, see col. 8, lines 40-45.

As per claim 45 and 49, Holloway's private key is doubly encrypted using PPu and a Consent phrase (CPu), see col. 8, lines 38-42 which provides an encrypted communication between the client and the key server, see col. 8, line 66 through col. 9, line 1, see also col. 9, lines 16-26, col. 7, lines 45-47.

As per claims 46 and 47, Holloway teaches that when applet Ap or browser terminate, the algorithms and keys are lost from the memory of client. This clearly suggests a volatile memory of the client system for storing decryption information and decrypted information recited in claims 46 and 47.

As per claim 50, Holloway teaches an authentication token (i.e. smart card) providing authentication information, see col. 8, lines 20-23, and an authentication server (i.e. system server) providing decryption information (i.e. such as an applet Ap), see 7, lines 50-53.

Claim Rejections - 35 USC § 102

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 11-13, 15-16 19, 21-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Kaufman et al., U.S. Pat. No. 5,491,752, published Feb. 1996.

As per claims 11-13, 15 and 19, 21-22, Kaufman is directed to an improved security system which inhibits eavesdropping, dictionary attack, and intrusion into stored password, see abstract.

Kaufman's invention is implemented in a computing network which includes an authentication server restricting unauthorized users from accessing the network and "authenticates" proper users of the network, see col. 8, lines 21-64.

Kaufman's authentication server is connected to a passive authentication generator which assists the authentication server in interacting with various users utilizing the services of the network. Each user of Kaufman's invention is provided with a workstation connected to a number of resources and each user is also provided with a passive authentication token generator to assist the user in interacting with the authentication server.

In operation, when a user verifies his identity to the server, the server provides the workstation with an encrypted message comprising a ticket useful in logging in a desired computing system .

Kaufman teaches that when user desires to access the desired computing system, the workstation receives the user name of the user which identifies the user to the network, the password of the user and a token obtained from the token generator. The workstation computes a transmission code based on the password and the token (, see col. 9, lines 15-61) and sends the transmission code to the server, see col. 10, lines 18-20.

Kaufman further teaches that the server encrypts a message (i.e. a ticket) using the session code as a secret key and transmits the encrypted ticket and a challenge (i.e. authentication information) to the workstation, see col. 12, lines 37-64, where the user inputs the received challenge into the token generator where a secret key is calculated to decrypt the

encrypted message (i.e. encrypted personal security device) as a ticket to gain access to the desired system for a selected period of time and a session-specific shared secret key to encrypt and decrypt subsequent communication with the desired system.

As per claims 16 and 23, Kaufman teaches that the transmission code is a time-dependent authentication information, see col.9 lines 31-40.

As per claim 24, Kaufman teaches that the server encrypts a message (i.e. a ticket) using the session code as a secret key and transmits the encrypted ticket and a challenge (i.e. authentication information) to the workstation, see col. 12, lines 37-64, where the user inputs the received challenge into the token generator where a secret key is calculated to decrypt the encrypted message (i.e. encrypted personal security device) as a ticket to gain access to the desired system.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 32, 38 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holloway as applied to claims 25, 33 and 42 above, and further in view of Kaufman U.S. Pat. No. 5,491,752, published Feb. 1996.

Holloway fails to teach time-dependent authentication information recited in claims 32, 38 and 51.

However, However, Kaufman teaches an authentication server connected to a passive authentication generator which assists the authentication server in interacting with various users utilizing the services of the network. Each user of Kaufman's invention is provided with a workstation connected to a number of resources and each user is also provided with a passive authentication token generator to assist the user in interacting with the authentication server.

In operation, when a user verifies his identity to the server, the server provides the workstation with an encrypted message comprising a ticket useful in logging in a desired computing system. see col. 8, lines 21-64.

Kaufman teaches a transmission code based on the password and the token (, see col. 9, lines 15-61) sent to the server, see col. 10, lines 18-20.

Kaufman's transmission code is a time-dependent authentication information, see col.9 lines 31-40.

It would have been obvious to one of ordinary skill in the art to adapt the Holloway's authentication information (i.e. PPu) to that of Kaufman's transmission code to include a time dependent authentication (i.e. an active token) code to further reduce dictionary attack known in password-based authentication, see col. 4, lines 21-38.

Allowable Subject Matter

Claims 4, 8,9,14, 17, 18, 20, 30, 31, 35, 40,41,43,48 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7240

Taghi Arani

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100